Federal Register

Monday,
May 2, 2005

Part II

National Credit Union Administration

12 CFR Part 748

Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice; Final Rule

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

AGENCY: National Credit Union Administration (NCUA).

ACTION: Final rule.

SUMMARY: NCUA is amending its rule governing security program elements to require federally insured credit unions to include response programs to address instances of unauthorized access to member information. NCUA is also including guidance, in the form of Appendix B, to provide federally insured credit unions with direction on ways to meet the new regulatory requirements.

DATES: This rule is effective on June 1, 2005.

FOR FURTHER INFORMATION CONTACT: Matthew J. Biliouris, Senior Information Systems Officer, Office of Examination & Insurance, Division of Supervision, at telephone (703) 518–6394; or Ross Kendall, Staff Attorney, Office of General Counsel, at telephone (703) 518–6562.

SUPPLEMENTARY INFORMATION: The contents of this preamble are listed in the following outline:

I. Introduction
II. Overview of the Comments Received
III. Overview of the Final Guidance
IV. Section-by-Section Analysis of the Comments Received
A. The ''Background'' Section
B. The ''Response Program'' Section
C. The ''Member Notice'' Section
V. Effective Date
VI. Impact of Guidance
VII. Regulatory Analysis
A. Paperwork Reduction Act
B. Regulatory Flexibility Act
C. Executive Order 12866
D. Unfunded Mandates Act of 1995

I. Introduction

In 2001, NCUA amended 12 CFR Part 748 to fulfill a requirement in Section 501 of the Gramm-Leach-Bliley Act (Pub. L. 106–102) (GLBA), in which Congress directed both NCUA and the other Federal Financial Institution Examination Council (FFIEC) agencies, including the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, the ''Banking Agencies'') to establish standards for financial institutions relating to administrative, technical, and physical safeguards to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Although NCUA worked with the Banking Agencies to develop the standards described above, the Banking Agencies issued their standards as guidelines under the authority of Section 39 of the Federal Deposit Insurance Act.

Since Section 39 of the Federal Deposit Insurance Act does not apply to NCUA, the NCUA Board determined that it could best meet the congressional directive to prescribe standards through an amendment to its existing regulation governing security programs for federally insured credit unions and by providing guidance to credit unions, substantially identical to the guidelines issued by the Banking Agencies, in an appendix to the regulation. 12 CFR Part 748, Appendix A; 66 FR 8152 (January 30, 2001). The preamble to the final rule discusses the different regulatory framework under which the Banking Agencies issued their guidelines. The final regulation requires each federally insured credit union to establish and maintain a security program implementing the safeguards required by GLBA.

Appendix A, entitled Guidelines for Safeguarding Member Information (Appendix A), is intended to outline industry best practices and assist credit unions to develop meaningful and effective security programs to ensure compliance with the requirements contained in the regulation. Among other things, Appendix A advises credit unions to: (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and (3) assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[1]

On October 23, 2003, the NCUA Board approved a proposal to revise 12 CFR Part 748 to include a requirement to respond to incidents of unauthorized access to member information. The Board invited comment on all aspects of the proposed Guidance. The public comment period closed on December 29, 2003.

This final rule further amends Part 748 to require that every federally insured credit union have a security program that contains a provision for responding to incidents of unauthorized access to member information. Appendix B, entitled Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, is also provided to assist credit unions in developing and maintaining their response programs. Appendix B describes NCUA's expectation that every federally insured credit union develop a response program, including member notification procedures, to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

NCUA has modified the proposed Guidance to provide credit unions with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations, while continuing to highlight member notice as a key feature of a credit union's response program. In addition, NCUA reorganized the proposed Guidance for greater clarity. A more detailed discussion of the changes follows.

II. Overview of Comments Received

NCUA received 15 comment letters on the proposed Guidance: Six from natural person credit unions, one from a corporate credit union, two from national credit union trade associations, five from state credit union leagues, and one from a service provider. In addition, the Banking Agencies collectively received 65 comment letters. While the NCUA Board carefully considered all comments on its proposed rule, to remain as consistent as practicable with the Banking Agencies, the Board has also made some changes in the final rule as a result of interagency discussions.

As a general matter, commenters agreed that credit unions should have response programs. Indeed, many credit unions and other financial institutions described having such programs in place. Many comments received commended the NCUA and the Banking Agencies for providing guidance on response programs. However, the majority of industry commenters criticized the prescriptive nature of the proposed Guidance. These commenters stated that the rigid approach in the proposed Guidance would stifle innovation and retard the effective evolution of response programs.

[1] 12 CFR Part 748, Appendix A, Paragraph III.B.2.

Industry commenters raised concerns that the specific requirements in the proposed Guidance would not permit a credit union to assess different situations from its own business perspective, specific to its size, operational and system structure, and risk tolerances.

Some industry commenters asserted that there is no need for regulation in this area and recommended that the NCUA and the Banking Agencies withdraw the proposed Guidance. Some of these commenters suggested, instead, that the Agencies re-issue the proposed Guidance as a best practices document. Other industry commenters suggested modifying the proposed Guidance to give credit unions greater discretion to determine how to respond to incidents of unauthorized access to or use of member information.

Two commenters also requested that the Agencies include a transition period allowing adequate time for financial institutions to implement the final Guidance. Some commenters asked for a transition period only for the aspects of the final Guidance that address service provider arrangements.

III. Overview of Final Guidance

The final rule requires that every federally insured credit union must develop and implement a response program designed to address incidents of unauthorized access to member information maintained by the credit union or its service provider. The final Guidance provides each credit union with greater flexibility to design a risk-based response program tailored to the size, complexity and nature of its operations.

The final Guidance, which has been reorganized for greater clarity, continues to highlight member notice as a key feature of a credit union's response program. However, in response to the comments received, the final Guidance modifies the standard describing when notice should be given and provides for a delay at the request of law enforcement. It also modifies which members should be given notice, what a notice should contain, and how it should be delivered.

A more detailed discussion of the final Guidance and the manner in which it incorporates comments NCUA and the Banking Agencies received follows.

IV. Section-by-Section Analysis of the Comments Received

A. The ''Background'' Section

Legal Authority

The legal foundation for the Guidance is set forth in Part 748, which derives from section 501(b) of GLBA and requires that every credit union have a security program. Appendix A to Part 748 describes the elements of a security program and includes measures to protect member information maintained by the credit union or its service providers. The Guidance states that NCUA expects member notification to be a component of such a response program.

One commenter questioned NCUA's and the Banking Agencies' legal authority to issue the Guidance. This commenter asserted that section 501(b) of GLBA only authorizes the Agencies to establish standards requiring financial institutions to safeguard the confidentiality and integrity of customer information and to protect that information from unauthorized access, but does not authorize standards that would require a response to incidents where the security of customer information actually has been breached.

The NCUA Board notes, however, that section 501(b)(3) specifically states that the standards to be established by the Agencies must include various safeguards to protect against not only ''unauthorized access to,'' but also, the ''use of'' customer information that could result in ''substantial harm or inconvenience to any customer.'' The NCUA Board determined that this language provides a legal basis for standards that include response programs to address incidents of unauthorized access to member information. Response programs represent the principal means for a credit union to protect against unauthorized ''use'' of member information that could lead to ''substantial harm or inconvenience'' to the member. For example, member notification is an important tool that enables a member to take steps to prevent identity theft, such as by arranging to have a fraud alert placed in his or her credit file.

Scope of Guidance

The proposed Guidance contained several cross references to definitions used in Appendix A. However, the NCUA Board did not specifically address the scope of the proposed Guidance. A number of commenters had questions and suggestions regarding the scope of the proposed Guidance and the meaning of terms used.

Entities and Information Covered

Some commenters had questions about the entities and information covered by the proposed Guidance. One commenter suggested that NCUA and the Banking Agencies clarify that foreign offices, branches, and affiliates of United States banks are not subject to the final Guidance. Another commenter wanted the NCUA Board to clarify corporate credit unions' responsibilities relating to the Guidance. This commenter wanted to know if corporate credit unions would be expected to follow the same practices of that of a service provider and notify affected natural person credit unions.

Some commenters recommended that the Agencies clarify that the final Guidance only applies to unauthorized access to sensitive information within the control of the financial institution. One commenter thought that the final Guidance should be broad and cover fraud committed against credit union members through the Internet, such as through the misuse of online corporate identities to defraud online banking users through fake web sites (commonly known as ''phishing''). Several commenters requested confirmation in the final Guidance that it applies to consumer accounts and not to business and other commercial accounts.

For greater clarity, NCUA has revised the Background section of the final Guidance to state that the scope and definitions of terms used in the Guidance are identical to those in section 501(b) of the GLBA and Appendix A, which largely cross-reference definitions used in NCUA's Privacy Rule.[2] Therefore, consistent with section 501(b) and Appendix A, this final Guidance applies to the entities enumerated in section 505(a) of the GLBA. This final Guidance does not apply to a credit union's foreign offices, branches, or CUSOs. However, a credit union is responsible for the security of its member information, whether the information is maintained within or outside of the United States, and whether or not it relies on a CUSO to provide certain member services.

As with the guidance contained in Appendix A, natural person credit unions that use corporate credit unions as their ''service providers'' will likely look to the final Guidance in overseeing their service provider arrangements with those corporate credit unions. Accordingly, there is no exemption for corporate credit unions that provide services to natural person credit unions as part of normal processing business.

The final Guidance also applies to ''member information,'' meaning any record containing ''nonpublic personal information'' (as that term is defined in section 716.3(n) of NCUA's Privacy rule) about a credit union's member, whether in paper, electronic, or other form, that

[2] 12 CFR Part 716.

is maintained by or on behalf of the institution.[3] Consequently, the final Guidance applies only to information that is within the control of the credit union and its service providers, and would not apply to information directly disclosed by a member to a third party, for example, through a fraudulent web site.

Moreover, the final Guidance does not apply to information involving business or commercial accounts. Instead, the final Guidance applies to nonpublic personal information about a ''member'' within the meaning of Appendix A, namely, a consumer who obtains a financial product or service from a credit union to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the credit union.[4]

Effect of Other Laws

Several commenters requested NCUA and the Banking Agencies explain how the final Guidance interacts with additional and possibly conflicting state law requirements. Most of these commenters urged that the final Guidance expressly preempt state law. By contrast, one commenter asked the Agencies to clarify that a financial institution must also comply with additional state law requirements. In addition, some commenters asked that the final Guidance provide a safe harbor defense against class action law suits. They suggested that the safe harbor should cover any credit union that takes reasonable steps that regulators require to protect member information, but, nonetheless, experiences an event beyond its control that leads to the disclosure of member information.

These issues do not fall within the scope of this final Guidance. The extent to which section 501(b) of GLBA, Appendix A, and any related NCUA interpretations, such as this final Guidance, preempts state law is governed by Federal law, including the procedures set forth in section 507 of GLBA, 15 U.S.C. 6807.[5] Moreover, there is nothing in Title V of the GLBA that authorizes NCUA to provide credit unions with a safe harbor defense. Therefore, the final Guidance does not address these issues.

Organizational Changes in the ''Background'' Section

For the reasons described earlier, the Background section is adopted essentially as proposed, except that the latter part of the paragraph on ''Service Providers'' and the entire paragraph on ''Response Programs'' are incorporated into the introductory discussion of Section II. The NCUA Board believes that the Background section is now clearer, as it focuses solely on the statutory and regulatory framework upon which the final Guidance is based. Comments and changes with respect to the paragraphs that were relocated are discussed in the next section.

B. The ''Response Program'' Section

There are a number of differences between the discussion of Response Programs in the proposed and final Guidance. The introduction to section II of the proposed Guidance stated that a response program should be a key part of a credit union's information security program required under Part 748. It also described the importance of having a response program and of timely notification of members when warranted. Section II of the proposed Guidance contained four detailed paragraphs describing each of the four components that a response program should contain.

The introductory language in the final Guidance now emphasizes that a credit union's response program should be risk-based and describes the components of a response program in a less prescriptive manner. Section II in the final Guidance specifically states that a credit union should implement security measures, from among the itemized list in Appendix A, designed to prevent unauthorized access to or use of member information, such as by placing access controls on member information systems and conducting background checks[6] for employees who are authorized to access member information. It then states that NCUA expects every credit union to develop and implement a risk-based response program (another security measure enumerated in Appendix A) designed to address incidents of unauthorized access to member information that occur despite measures to prevent security breaches. The final Guidance also states that a response program should be a key part of a credit union's information security program.

This introductory paragraph is intended to make clear that, based upon the prevalence of identity theft in the United States,[7] every credit union should have a response program to be prepared to prevent and address attempts to gain unauthorized access to its member information. The Board's expectation that each credit union will develop a response program is consistent with the provision in Appendix A calling for each credit union to design an information security program to control ''identified risks'' stemming from ''reasonably foreseeable internal and external threats.''[8]

Service Provider Contracts

The Background section of the proposed Guidance elaborated on the specific provisions that a credit union's contracts with its service providers should contain. The proposed Guidance stated that a credit union's contract with its service provider should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. It stated that this disclosure would permit a credit union to expeditiously implement its response program.

Several commenters on the proposed Guidance agreed that a credit union's contracts with its service providers should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. However, many commenters suggested modifications to this provision.

The discussion of this aspect of a credit union's contracts with its service providers is in section II of the final Guidance. It has been revised as follows in response to the comments received.

Timing of Service Provider Notification

NCUA and the Banking Agencies received a number of comments regarding the timing of a service

[3] *See* 12 CFR Part 745, Appendix A, Paragraph I.C.2.c.

[4] *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.b.; 12 CFR Part 716.3(i).

[5] Section 507 provides that state laws that are ''inconsistent'' with the provisions of Title V, Subtitle A of the GLBA are preempted ''only to the extent of the inconsistency.'' State laws are ''not consistent'' if they offer greater protection than Subtitle A, as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under Section 505(a) of either the person that initiated the complaint or that is the subject of the complaint. *See* 15 U.S.C. 6807.

[6] A footnote has been added to this section to make clear that credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[7] See, for example, the Federal Trade Commission's Identity Theft Survey Report of September 2003,'' available at *http://www.ftc.gov/os/2003/09synovatereport.pdf* estimating that 10 million Americans were victims of identify theft in 2002.

[8] 12 CFR Part 748, Appendix A, Paragraph III.B. and III.C.

provider's notice to a credit union. One commenter suggested requiring service providers to report incidents of unauthorized access to credit unions within 24 hours after discovery of the incident.

In response to comments on the timing of a service provider's notice to a credit union, the final Guidance states that a credit union's contract with its service provider should require the service provider to take appropriate action to address incidents of unauthorized access to the credit union's member information, including notifying the credit union as soon as possible of any such incident, to enable the credit union to expeditiously implement its response program. The NCUA Board determined that requiring notice within 24 hours of an incident may not be practicable or appropriate in every situation, particularly where, for example, it takes a service provider time to investigate a breach in security. Therefore, the final Guidance does not specify a number of hours or days by which the service provider must give notice to the credit union.

Existing Contracts With Service Providers

Some commenters expressed concerns that they would have to rewrite their contracts with service providers to require the disclosure described in this provision. These commenters asked NCUA to grandfather existing contracts and to apply this provision only prospectively to new contracts. Many commenters also suggested that the final Guidance contain a transition period to permit credit unions to modify their existing contracts.

The NCUA Board has decided not to grandfather existing contracts or to add a transition period to the final Guidance because, as stated in the proposed Guidance, this disclosure provision is consistent with the obligations in Appendix A that relate to service provider arrangements and with existing guidance on this topic previously issued by NCUA.[9] In order to ensure the safeguarding of member information, credit unions that use service providers likely have already arranged to receive notification from the service providers when member information is accessed in an unauthorized manner. In light of the comments received, however, NCUA recognizes that there are credit unions that have not formally included such a disclosure requirement in their contracts. Where this is the case, the credit union should exercise its best efforts to add a disclosure requirement to its contracts and any new contracts should include such a provision.

Thus, the final Guidance adopts the discussion on service provider arrangements largely as proposed. To eliminate any ambiguity regarding the application of this section to foreign-based service providers, however, the final Guidance now makes clear that a covered credit union[10] should be capable of addressing incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers.[11]

Components of a Response Program

As described earlier, commenters criticized the prescriptive nature of proposed Section II that described the four components a response program should contain. The proposed Guidance instructed credit unions to design programs to respond to incidents of unauthorized access to member information by (1) assessing the situation; (2) notifying regulatory and law enforcement agencies; (3) containing and controlling the situation; and (4) taking corrective measures. The proposed Guidance contained detailed information about each of these four components.

The introductory discussion in this section of the final Guidance now makes clear that, as a general matter, a credit union's response program should be risk-based. It applies this principle by modifying the discussion of a number of these components. The NCUA Board determined that the detailed instructions in these components of the proposed Guidance, especially in the ''Corrective Measures'' section, would not always be relevant or appropriate. Therefore, the final Guidance describes, through brief, bulleted points, the elements of a response program, giving credit unions greater discretion to address incidents of unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

At a minimum, a credit union's response program should contain procedures for (1) assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused; (2) notifying the appropriate NCUA Regional Director and, in the case of state-chartered credit unions, its applicable state supervisory agency as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information, as defined in the final Guidance, (3) immediately notifying law enforcement authorities in situations involving Federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying members when warranted.

Assess the Situation

The proposed Guidance stated that a credit union should assess the nature and scope of the incident and identify what member information systems and types of member information have been accessed or misused.

Some commenters stated that NCUA and the Banking Agencies should retain this provision in the final Guidance. One commenter suggested that a credit union should focus its entire response program primarily on addressing unauthorized access to sensitive member information.

The NCUA Board has concluded that a credit union's response program should begin with a risk assessment that allows a credit union to establish the nature of any information improperly accessed. This will allow the credit union to determine whether and how to respond to an incident. Accordingly, the NCUA Board has not changed this provision.

Notify Regulatory and Law Enforcement Agencies

The proposed Guidance provided that a credit union should promptly notify NCUA when it becomes aware of an incident involving unauthorized access to or use of member information that could result in substantial harm or inconvenience to members. To clarify its expectations, the NCUA Board has amended the bullet point addressing notification of the regulator to include notification of the appropriate NCUA Regional Director, as well as any applicable state supervisory agency in the case of state-chartered credit unions.

In addition, the proposed Guidance stated that a credit union should file a Suspicious Activity Report (SAR), if required, in accordance with 12 CFR

[9] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, June 2004; NCUA Letter to Credit Unions No. 00–CU–11, December 2000.

[10] *See* footnote 5, *supra*.

[11] *See e.g.*, FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, June 2004.

Part 748 and various NCUA issuances.[12] The proposed Guidance stated that, consistent with the NCUA's SAR regulation, in situations involving Federal criminal violations requiring immediate attention, the credit union immediately should notify, by telephone, the appropriate law enforcement authorities and its primary regulator, in addition to filing a timely SAR. For the sake of clarity, the final Guidance discusses notice to regulators and notice to law enforcement in two separate, bulleted items.

Standard for Notice to Regulators

The provision regarding notice to regulators in the proposed Guidance prompted numerous comments. Many commenters suggested that NCUA adopt a narrow standard for notifying regulators. These commenters were concerned that notice to regulators, provided under the circumstances described in the proposed Guidance, would be unduly burdensome for credit unions, service providers, and regulators, alike.

Some of these commenters suggested that NCUA adopt the same standard for notifying regulators and members. These commenters recommended that notification occur when a credit union becomes aware of an incident involving unauthorized access to or use of ''sensitive member information,'' a defined term in the proposed Guidance that specified a subset of member information deemed by NCUA as most likely to be misused.

Other commenters recommended that the Agencies narrow this provision so that a credit union will inform a regulator only in connection with an incident that poses a significant risk of substantial harm to a significant number of its members, or only in a situation where substantial harm to members has occurred or is likely to occur, instead of when it could occur.

Other commenters who advocated the adoption of a narrower standard asked NCUA to take the position that filing an SAR constitutes sufficient notice and that notification of other regulatory and law enforcement agencies is at the sole discretion of the credit union. One commenter stated that it is difficult to imagine any scenario that would trigger the response program without requiring a SAR filing. Some commenters asserted that if NCUA believes a lower threshold is advisable for security breaches, it should amend Part 748.

By contrast, some commenters recommended that the standard for notification of regulators remain broad. One commenter advocated that any event that triggers an internal investigation by the credit union should require notice to the appropriate regulator. Another commenter similarly suggested that notification of all security events to federal regulators is critical, not only those involving unauthorized access to or use of member information that could result in substantial harm or inconvenience to its members.

The NCUA Board has concluded that the standard for notification to regulators should provide an early warning to allow NCUA or applicable state supervisory agency to assess the effectiveness of a credit union's response plan, and, where appropriate, to direct that notice be given to members if the credit union has not already done so. Thus, the standard in the final Guidance states that a credit union should notify its primary regulator as soon as possible if the credit union becomes aware of an incident involving unauthorized access to or use of ''sensitive member information.''

''Sensitive member information'' is defined in section III of the final Guidance and means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. ''Sensitive member information'' also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

This standard is narrower than that in the proposed Guidance because a credit union will need to notify NCUA when, and only if, it becomes aware of an incident involving ''sensitive member information.'' Therefore, under the final Guidance, there will be fewer occasions when a credit union should need to notify NCUA. However, under this standard, a credit union will need to notify NCUA at the time that the credit union initiates its investigation to determine the likelihood that the information has been or will be misused, so that NCUA will be able to take appropriate action, if necessary.

Notice to Regulators by Service Providers

Commenters on the proposed Guidance questioned whether a credit union or its service provider should give notice to a regulator when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider. One commenter noted that if a security event occurs at a large service provider, regulators could receive thousands of notices from institutions relating to the same event. The commenter suggested that if a service provider is examined by one of the Agencies the most efficient means of providing regulatory notice of such a security event would be to allow the servicer to notify its primary Agency contact. The primary Agency contact then could disseminate the information to the other regulatory agencies as appropriate.

The NCUA Board believes it is the responsibility of the credit union and not the service provider to notify NCUA. Therefore, the final Guidance states that a credit union should notify NCUA as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information. Nonetheless, a security incident at a service provider could have an impact on multiple financial institutions that are supervised by different Federal regulators. Therefore, in the interest of efficiency and burden reduction, the last paragraph in section II of the final Guidance makes clear that a credit union may authorize or contract with its service provider to notify the NCUA on the credit union's behalf when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider.

Notice to Law Enforcement

Some commenters took issue with the provision in the proposed Guidance regarding notification of law enforcement by telephone. One interagency commenter asked the Banking Agencies to clarify how notification of law enforcement by telephone would work since in many cases it is unclear what telephone number should be used. This commenter maintained that size and sophistication of law enforcement authorities may differ from state to state and this requirement may create confusion and unwarranted action by the law enforcement authority.

The final Guidance adopts this provision as proposed. The NCUA

[12] *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspicious Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Issues, Issue 6, November 2003, February 2004.

Board notes that the provision stating that a credit union should notify law enforcement by telephone in situations involving federal criminal violations requiring immediate attention is consistent with Part 748.

Contain and Control the Situation

The proposed Guidance stated that the credit union should take measures to contain and control a security incident to prevent further unauthorized access to or use of member information while preserving records and other evidence.[13] It also stated that, depending upon the particular facts and circumstances of the incident, measures in connection with computer intrusions could include: (1) Shutting down applications or third party connections; (2) reconfiguring firewalls in cases of unauthorized electronic intrusion; (3) ensuring that all known vulnerabilities in the credit union's computer systems have been addressed; (4) changing computer access codes; (5) modifying physical access controls; and (6) placing additional controls on service provider arrangements.

Few comments were received on this section. One interagency commenter suggested that the Banking Agencies adopt this section unchanged in the final Guidance. Another commenter had questions about the meaning of the phrase ''known vulnerabilities.'' Commenters did, however, note the overlap between proposed section II.C and the corrective measures in proposed section II.D, described as ''flagging accounts'' and ''securing accounts.''

NCUA and the Banking Agencies agree that some sections in the proposed Guidance overlapped. Therefore, the NCUA Board modified this section by incorporating concepts from the proposed Corrective Measures component, and removing the more specific examples in this section, including the terms that confused commenters. This section in the final Guidance gives a credit union greater discretion to determine the measures it will take to contain and control a security incident. It states that credit unions should take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, such as, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.

Preserving Evidence

One interagency commenter stated that the final Guidance should require financial institutions, as part of the response process, to have an effective computer forensics capability in order to investigate and mitigate computer security incidents as discussed in principle fourteen of the Basel Committee's ''Risk Management for Electronic Banking''[14] and the International Organization for Standardization's ISO 17799.[15]

The NCUA Board notes that the final Guidance addresses not only computer security incidents, but also all other incidents of unauthorized access to member information. Thus, the Board thinks it is not appropriate to include more detail about steps a credit union should take to investigate and mitigate computer security incidents. However, the NCUA Board believes that credit unions should be mindful of industry standards when investigating an incident. Therefore, the final Guidance contains a reference to forensics by generally noting that a credit union should take appropriate steps to contain and control an incident, while preserving records and other evidence.

Corrective Measures

The proposed Guidance stated that once a credit union understands the scope of the incident and has taken steps to contain and control the situation, it should take measures to address and mitigate the harm to individual members. It then described three corrective measures that a credit union should include as a part of its response program in order to effectively address and mitigate harm to individual members: (1) Flagging accounts; (2) securing accounts; and (3) notifying members. The NCUA Board removed the first two corrective measures for the reasons that follow.

Flagging and Securing Accounts

The first corrective measure in the proposed Guidance directed credit unions to ''flag accounts.'' It stated that a credit union should immediately begin identifying and monitoring the accounts of those members whose information may have been accessed or misused. It also stated that a credit union should provide staff with instructions regarding the recording and reporting of any unusual activity, and if indicated given the facts of a particular incident, implement controls to prevent the unauthorized withdrawal or transfer of funds from member accounts.

The second corrective measure directed credit unions to ''secure accounts.'' The proposed Guidance stated that when a share draft, savings, or other member account number, debit or credit card account number, personal identification number (PIN), password, or other unique identifier has been accessed or misused, the credit union should secure the account and all other accounts and services that can be accessed using the same account number or name and password combination. The proposed Guidance stated that accounts should be secured until such time as the credit union and the member agree on a course of action.

Commenters were critical of these proposed measures. Several commenters asserted that the final Guidance should not prescribe responses to security incidents with this level of detail. Other commenters recommended that if NCUA chooses to retain references to ''flagging'' or ''securing'' accounts, it should include the words ''where appropriate'' in order to give credit unions the flexibility to choose the most effective solutions to problems.

Commenters also stated that the decision to flag accounts, the nature of the flag, and the duration of the flag, should be left to an individual credit union's risk-based procedures developed under Appendix A. These commenters asked NCUA to recognize that regular, ongoing fraud prevention and detection methods employed by a credit union may be sufficient.

Commenters representing small credit unions stated that they do not have the technology or other resources to monitor individual accounts. They stated that the financial impact of having to monitor accounts for unusual activity would be enormous, as each credit union would have to purchase expensive technology, hire more personnel, or both. These commenters asked NCUA to provide credit unions with the flexibility to close an account if the credit union detects unusual activity.

With respect to ''securing accounts,'' several commenters stated that if ''secure'' means close or freeze, either is extreme and would have significant adverse consequences for members. Other commenters stated that the requirement that the credit union and the member ''agree on a course of action'' is unrealistic, unworkable and should be eliminated. Some commenters explained that if a member is traveling and the credit union cannot contact the member to obtain the member's consent, freezing or closing a

[13] *See* FFIEC Information Security Booklet, December. 2002, pp. 68–74, avaialble at *http://www.ffiec.gov/ffiecinfobase.html_pages/it_01.html#infosec.*

[14] *http://www.bis.org/publ/bcbs35.htm.*

[15] *http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html.*

member's account could strand the member with no means of taking care of expenses. They stated that, in the typical case, the credit union would monitor such an account for suspicious transactions.

As described earlier, the NCUA Board is adopting an approach in the final Guidance that is more flexible and risk-based than that in the proposed Guidance. The final Guidance incorporates the general concepts described in the first two corrective measures into the brief bullets describing components of a response program enumerated in section II.C. Therefore, the first and second corrective measures no longer appear in the Guidance.

Member Notice and Assistance

The third corrective measure in the proposed Guidance is titled ''Member Notice and Assistance.'' This proposed measure stated that a credit union should notify and offer assistance to members whose information was the subject of an incident of unauthorized access or use under the circumstances described in section III of the proposed Guidance. The proposed Guidance also described which members should be notified. In addition, this corrective measure contained provisions discussing delivery and contents of the member notice.

The final Guidance now states that a credit union's response program should contain procedures for notifying members when warranted. For clarity's sake, the discussion of which members should be notified, and the delivery and contents of member notice, is now in new section III, titled ''Member Notice.'' Comments and changes with respect to the paragraphs that were relocated are discussed under the section titled ''Member Notice'' that follows.

Responsibility for Notice to Members

Some commenters were confused by the discussion in the proposed Guidance stating that a credit union's contract with its service provider should require the service provider to disclose fully to the credit union information related to any breach in security resulting in an unauthorized intrusion into the credit union's member information systems maintained by the service provider. Commenters stated that this provision appears to create an obligation for both credit unions and their service providers to provide notice of security incidents to the credit union's members. These commenters recommended that the service provider notify its credit union customer so that the credit union can provide appropriate notice to its members. Thus, members would avoid receiving multiple notices relating to a single security incident.

Other commenters asserted that a credit union should not have to notify its members if an incident has occurred because of the negligence of its service provider. These commenters recommended that in this situation, the service provider should be responsible for providing notice to the credit union's members.

As discussed above in connection with notice to regulators, the NCUA Board believes that it is the responsibility of the credit union, and not of the service provider, to notify the credit union's members in connection with an unauthorized intrusion into a credit union's member information systems maintained by the service provider. The responsibility to notify members remains with the credit union whether the incident is inadvertent or due to the service provider's negligence. The NCUA Board notes that the costs of providing notice to the credit union's members as a result of negligence on the part of the service provider may be addressed in the credit union's contract with its service provider.

The last paragraph in section II of the final Guidance, therefore, states that it is the responsibility of the credit union to notify the credit union's members. It also states that the credit union may authorize or contract with its service provider to notify members on the credit union's behalf when a security incident involves an unauthorized intrusion into the credit union's member information systems maintained by the service provider.

C. The ''Member Notice'' Section

Section III of the proposed Guidance described the standard for providing notice to members and defined the term ''sensitive member information'' used in that standard. This section also gave examples of circumstances when a credit union should give notice and when NCUA does not expect a credit union to give notice. It also discussed contents of the notice and proper delivery.

Section III of the final Guidance contains a more comprehensive discussion of member notice. It describes the standard for providing notice to members and defines both the terms ''sensitive member information'' and ''affected members.'' It also discusses the contents of the notice and proper delivery.

Standard for Providing Notice

A key feature of the proposed Guidance was the description of when a credit union should provide member notice. The proposed Guidance stated that a credit union should notify affected members whenever it becomes aware of unauthorized access to ''sensitive member information'' unless the credit union, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including by monitoring affected members' accounts for unusual or suspicious activity.

The NCUA Board proposed this standard as a way to strike a balance between notification to members every time the mere possibility of misuse of member information arises from unauthorized access and a situation where the credit union knows with certainty that information is being misused. However, the Board specifically requested comment on whether this is the appropriate standard and invited commenters to offer alternative thresholds for member notification.

Some commenters stated that the proposed standard was reasonable and sufficiently flexible. However, many commenters recommended that the Board provide credit unions with greater discretion to determine when a credit union should notify its members. Some of these commenters asserted that a credit union should not have to give notice unless the credit union believes it ''to be reasonably likely,'' or if circumstances indicated ''a significant risk'' that the information will be misused.

Commenters maintained that because the proposed standard states that a credit union should give notice when fraud or identity theft is merely possible, notification under these circumstances would needlessly alarm members where little likelihood of harm exists. Commenters claimed that, eventually, frequent notices in non-threatening situations will be perceived by members as routine and commonplace, and therefore reduce their effectiveness.

The NCUA Board believes that articulating as part of the Guidance a standard that sets forth when notice to members is warranted is both helpful and appropriate. However, the Board agrees with commenters and is concerned that the proposed threshold inappropriately required credit unions to prove a negative proposition, namely, that misuse of the information accessed

is unlikely to occur. In addition, the Board does not want members of credit unions to receive notices that would not be useful to them. Therefore, the NCUA Board has revised the standard for members notification.

The final Guidance provides that when a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused. If the credit union determines that misuse of the information has occurred or is reasonably possible, it should notify affected members as soon as possible.

An investigation is an integral part of the standard in the final Guidance. A credit union should not forego conducting an investigation to avoid reaching a conclusion that member information has been or will be misused and cannot unreasonably limit the scope of the investigation. However, the NCUA Board acknowledges that a full-scale investigation may not be necessary in all cases, such as where the facts readily indicate that information will or will not be misused.

Monitoring for Suspicious Activity

The proposed Guidance stated that a credit union need not notify members if it reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected members, including by monitoring affected members' accounts for unusual or suspicious activity. A number of comments addressed the standard in the proposed Guidance on monitoring affected members' accounts for unusual or suspicious activity.

Some commenters stated that the final Guidance should grant credit unions the discretion to monitor the affected member accounts for a period of time and to the extent warranted by the particular circumstances. Some commenters suggested that monitoring occur during the investigation. One commenter noted that a credit union's investigation may reveal that monitoring is unnecessary. One commenter noted that monitoring the member's accounts at the credit union may not protect the member, because unauthorized access to member information may result in identity theft beyond the accounts held at the specific credit union.

The NCUA Board agrees that under certain circumstances, monitoring may be unnecessary, for example when, on the basis of a reasonable investigation, a credit union determines that information was not misused. The Board also agrees that the monitoring element may not protect the member. Indeed, an identity thief with unauthorized access to certain sensitive member information likely will open accounts at other financial institutions in the member's name.

Accordingly, the Board concludes that monitoring under the circumstances described in the standard for notice would be burdensome for credit unions without a commensurate benefit to members. For these reasons, the Board has removed the reference to monitoring in the final Guidance.

Timing of Notice

The proposed Guidance did not include specific language on the timing of notice to members, and NCUA and the Banking Agencies received many comments on this issue. Some commenters requested clarification of the time frame for member notice. One commenter recommended that NCUA adopt the approach in the proposed Guidance because it does not set forth any circumstances that may delay notification of the affected members. Another commenter maintained that, in light of a member's need to act expeditiously against identity theft, an outside limit of 48 hours after the credit union learns of the breach is a reasonable and timely requirement for notice to members. Many commenters, however, recommended that NCUA make clear that a credit union may take the time it reasonably needs to conduct an investigation to assess the risk resulting from a security incident.

The NCUA Board has responded to these various comments on the timing of notice by providing that a credit union notify an affected member ''as soon as possible'' after concluding that misuse of the member's information has occurred, or is reasonably possible. As the scope and timing of a credit union's investigation is dictated by the facts and circumstances of a particular case, the Board has not designated a specific number of hours or days by which credit unions should provide notice to members. The Board believes that doing so may inhibit a credit union's ability to investigate adequately a particular incident or may result in notice that is not timely.

Delay for Law Enforcement Investigation

The proposed Guidance did not address delay of notice to members while a law enforcement investigation is conducted. Many commenters recommended permitting a credit union to delay notification to members to avoid compromising a law enforcement investigation. These commenters noted that the California Database Protection Act of 2003 (CDPA) requires notification of California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[16] However, the CDPA permits a delay in notification if a law enforcement agency determines that the notification will impede a criminal investigation.[17] Another commenter suggested that a credit union should not have to obtain a formal determination from a law enforcement agency before it is able to delay notice.

The NCUA Board agrees that it is appropriate to delay member notice if such notice will jeopardize a law enforcement investigation. However, to ensure that such a delay is necessary and justifiable, the final Guidance states that member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay.[18]

The NCUA Board is concerned that a delay of notification for a law enforcement investigation could interfere with the ability of members to protect themselves from identity theft and other misuse of their sensitive information. Thus, the final Guidance also provides that a credit union should notify its members as soon as notification will no longer interfere with the investigation and should maintain contact with the law enforcement agency that has requested a delay, in order to learn, in a timely manner, when member notice will no longer interfere with the investigation.

Sensitive Member Information

Scope of Standard

The Banking Agencies received many comments on the limitation of notice in the proposed Guidance to incidents involving unauthorized access to sensitive customer information. The NCUA Board invited comment on whether to modify the proposed standard for notice to apply to other circumstances that compel a credit union to conclude that unauthorized access to information, other than sensitive member information, likely

[16] The CDPA, also known as CA S.B. 1386, amended the Information Practices Act of 1977, California Civil Code, section 1798.82.

[17] *See* California Civil Code, section 1798.29(c).

[18] This includes circumstances when a credit union confirms that an oral request for delay from law enforcement will be followed by a written request.

will result in substantial harm or inconvenience to the affected members.

Most commenters recommended that the standard remain as proposed rather than covering other types of information. One interagency commenter suggested that the Agencies continue to allow a financial institution the discretion to notify affected customers in any other extraordinary circumstances that compel it to conclude that unauthorized access to information other than sensitive customer information likely will result in substantial harm or inconvenience to those affected. However, the commenter did not provide any examples of such extraordinary circumstances.

The NCUA Board continues to believe that the rationale for limiting the standard to sensitive member information expressed in the proposed Guidance is correct. The proposed Guidance explained that, in accordance with Appendix A, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. Substantial harm or inconvenience is most likely to result from improper access to sensitive member information because this type of information is easily misused, as in the commission of identity theft.

The NCUA Board has not identified any other circumstances that should prompt member notice and continues to believe that it is not likely that a member will suffer substantial harm or inconvenience from unauthorized access to other types of information. Therefore, the standard in the final Guidance continues to be limited to unauthorized access to sensitive member information. Of course, a credit union still may send notices to members in any additional circumstances that it determines are appropriate.

Definition of Sensitive Member Information

NCUA received many comments on the proposed definition of ''sensitive member information'' in the proposed Guidance. The first part of the proposed definition stated that ''sensitive member information'' is a member's social security number, personal identification number (PIN), password or account number, in conjunction with a personal identifier such as the member's name, address, or telephone number. The second part of the proposed definition stated that ''sensitive member information'' includes any combination of components of member information that allow someone to log onto or access another person's account, such as user name and password.

Some commenters agreed with this definition of ''sensitive member information.'' They said that it was sound, workable, and sufficiently detailed. However, many commenters proposed additions, exclusions, or alternative definitions.

Additional Elements

Some commenters suggested that NCUA add various data elements to the definition of sensitive member information, including: A driver's license number or number of other government-issued identification, mother's maiden name, and date of birth. One commenter suggested inclusion of other information that credit unions maintain in their member information systems such as a member's account balance, account activity, purchase history, and investment information. The commenter noted that misuse of this information in combination with a personal identifier can just as easily result in substantial harm or inconvenience to a member.

The NCUA Board has added to the first part of the definition several more specific components, such as driver's license number and debit and credit card numbers, because this information is commonly sought by identity thieves. However, the Board determined that the second part of the definition would cover the remaining suggestions. For example, where date of birth or mother's maiden name are used as passwords, under the final Guidance they will be considered components of member information that allow someone to log onto or access another person's account. Therefore, these specific elements have not been added to the definition.

Exclusions

Commenters also asserted that the proposed definition of sensitive member information is too broad and proposed various exclusions. For example, some commenters asked NCUA to exclude publicly available information, and also suggested that the final Guidance apply only to account numbers for transaction accounts or other accounts from which withdrawals or transfers can be initiated. These commenters explained that access to a mortgage account number (which may also be a public record) does not permit withdrawal of additional funds or otherwise damage the member. Other commenters requested that NCUA exclude encrypted information. Some of these commenters noted that only unencrypted information is covered by the CDPA.[19]

The final Guidance does not adopt any of the proposed exclusions. The NCUA Board believes it would be inappropriate to exclude publicly available information from the definition of sensitive member information, where publicly available information is otherwise covered by the definition of ''member information.''[20] So for instance, while a personal identifier, *i.e.,* name, address, or phone number, may be publicly available, it is sensitive member information when linked with particular nonpublic information such as a credit card account number. However, where the definition of ''member information'' does not cover publicly available information, sensitive member information also would not cover publicly available information. For instance, where an individual's name or address is linked with a mortgage loan account number that is in the public record, and therefore, would not be considered ''member information,''[21] it also would not be considered sensitive member information for purposes of the final Guidance.

In addition, access to a member's personal information and account number, whether or not it is an account from which withdrawals or transfers can be initiated, may permit an identity thief to access other accounts from which withdrawals can be made. Thus, the NCUA Board has determined that the definition of account number should not be limited as suggested by commenters. The Board also believes that a blanket exclusion for all encrypted information is not appropriate, because there are many levels of encryption, some of which do not effectively protect member information.

Alternative Definitions

Most alternative definitions suggested by commenters resembled the definition of ''personal information'' under the CDPA.[22] Under the CDPA, ''personal information'' includes a resident of California's name together with an account number, or credit or debit card

[19] *See* California Civil Code, 1798.29(a).

[20] *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.c.

[21] *See* 12 CFR § 716.3(p)(3)(i).

[22] Under the California law requiring notice, ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) driver's license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code access code, or password that would permit access to an individual's financial account.

number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. Therefore, some commenters asked that the final Guidance clarify that a name and an account number, together, is not sensitive member information unless these elements are combined with other information that permits access to a member's financial account.

The NCUA Board concluded that it would be helpful if credit unions could more easily compare and contrast the definition of ''personal information'' under the CDPA with the definition of ''sensitive information'' under the final Guidance. Therefore, the elements in the definition of sensitive information in the final Guidance are re-ordered and the Board added the elements discussed earlier.

The final Guidance states that sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. The final Guidance also states that sensitive member information includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or a password and account number.

Consistent with the Banking Agencies, the NCUA Board declines to adopt the CDPA standard for several reasons. First, for example, under the CDPA, personal information includes a person's name in combination with other data elements. By contrast, the final Guidance treats address and telephone number in the same manner as a member's name, because reverse directories may permit an address or telephone number to be traced back to an individual member.

In addition, under the CDPA, ''personal information'' includes name together with an account number, or credit or debit card number only if the information accessed also includes any required security code, access code, or password that would permit access to an individual's financial account. The NCUA Board notes that a name and account number, alone, is sufficient to create fraudulent checks, or to direct the unauthorized debit of a member's account even without an access code.[23] Further, a name and credit card number may permit unauthorized access to a member's account. Therefore, the final Guidance continues to define a member's name and account number, or credit or debit card number as sensitive member information.

Affected Customers

The NCUA Board also reviewed many interagency comments on the definition of ''affected members'' in the proposed Guidance. Section II.D.3 of the proposed Guidance provided that if the credit union could determine from its logs or other data precisely which members' information was accessed or misused, it may restrict its notification to those individuals. However, if the credit union cannot identify precisely which members were affected, it should notify each member in any group likely to have been affected, such as each member whose information is stored in the group of files in question.

Commenters were concerned that this provision in the proposed Guidance was overly broad. These commenters stated that providing notice to all members in groups likely to be affected would result in many notices that are not helpful. The commenters suggested that the final Guidance narrow the standard for notifying members to only those members whose information has been or is likely to be misused.

The discussion of ''affected members'' has been relocated and is separately set forth following the definition of ''sensitive member information'' in the final Guidance. The discussion of ''affected members'' in the final Guidance states that if a credit union, based upon its investigation, can determine from its logs or other data precisely which member's information has been improperly accessed,[24] it may notify only those members with respect to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, the final Guidance further notes that there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information contained in the group of files is reasonably possible, it should notify all members in the group. In this way, the final Guidance reduces the number of notices that should be sent.

Examples

The proposed Guidance described several examples of when a credit union should give notice and when NCUA does not expect a credit union to give notice.

NCUA received a number of comments on the examples. Some commenters thought the examples were helpful and suggested that NCUA add more. Other commenters criticized the examples as too broad. Many commenters suggested numerous ways to modify and clarify the examples.

Since the examples in the proposed Guidance led to interpretive questions, rather than interpretive clarity, the NCUA Board concluded that it is not particularly helpful to offer examples of when notice is and is not expected. In addition, the Board believes that the standard for notice itself has been clarified and examples are no longer necessary. Therefore, there are no examples in the final Guidance.

Content of Member Notice

NCUA received many comments on the discussion of the content of member notice located in section II.D.3.b of the proposed Guidance. The proposed Guidance stated that a notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It stated that the notice should also include a number that members can call for further information and assistance, remind members of the need to remain vigilant over the next 12 to 24 months, and recommend that members promptly report incidents of suspected identity theft. The proposed Guidance described several ''key elements'' that a notice should contain. It also provided a number of ''optional elements'' namely, examples of additional assistance that financial institutions have offered.

Some commenters agreed that the proposed Guidance sufficiently addressed most of the key elements necessary for an effective notice. However, many commenters requested greater discretion to determine the content of the notices that credit unions provide to members. Commenters suggested that NCUA make clear that the various items suggested for inclusion in any member notice are

[23] *See, e.g.,* Griff Witte, *Bogus Charges, Unknowingly Paid: FTC Accuses 2 of Raiding 90,000 Bank Accounts in Card Fraud,* Washington Post, May 29, 2004, at E1 (list of names with associated checking account numbers used by bogus company to debit bank accounts without customer authorization).

[24] NCUA notes that system logs may permit a credit union to determine precisely which members' data has been improperly accessed. *See, e.g.,* FFIEC Information Security Booklet, page 64, available at *http://www.ffiec.gov/ffiecinfobase.html_pages/it_01.html#infosec.*

suggestions, and that not every item is mandatory in every notice.

Some commenters took issue with the enumerated items in the proposed Guidance identified as key elements that a notice should contain. For example, many commenters asserted that members should not necessarily be encouraged to place fraud alerts with credit bureaus in every circumstance. Some of these commenters noted that not all situations will warrant having a fraud alert posted to the member's credit file, especially if the credit union took appropriate action to render the information accessed worthless. According to these commenters, the consequences of a fraud alert, such as increased obstacles to obtaining credit, may outweigh any benefit. Some commenters also noted that a proliferation of fraud alerts not related to actual fraud would dilute the effectiveness of the alerts.

Other commenters criticized the optional elements in the proposed Guidance. For instance, some commenters stated that a notice should not inform the member about subscription services that provide notification to the member when there is a request for the member's credit report, or offer to subscribe the member to this service, free of charge, for a period of time. These commenters asserted that member notices should not be converted into a marketing opportunity for subscription services provided by consumer credit bureaus. They stated that offering the service may mislead the member into believing that these expensive services are essential. If the service is offered free of charge, a credit union's choice of service could be interpreted as an endorsement for a specific company and its product.

As a result of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108–159, 117 Stat. 1985–86 (the FACT Act), many of the descriptions of ''key elements'' and ''optional elements'' in the proposed Guidance, and comments on these elements, have been superceded. For example, the frequency and circumstances under which a member may obtain a credit report free-of-charge have changed.

The final Guidance continues to specify that a notice should describe the incident in general terms and the member's information that was the subject of unauthorized access or use. It also continues to state that the notice should include a telephone number that members can call for further information and assistance, remind members of the need to remain vigilant over the next 12 to 24 months, and recommend that members promptly report incidents of suspected identity theft. In addition, the final Guidance also states that the notice should generally describe what the credit union has done to protect the members' information from further unauthorized access.

However, the final Guidance no longer distinguishes between certain other ''key'' items that the notice should contain and those that are ''optional.'' The NCUA Board added greater flexibility to this section to accommodate any new protections afforded to consumers that flow from the FACT Act. Instead of distinguishing between items that the notice should contain and those that are optional, a credit union may now select those items that are appropriate under the circumstances, and that are compatible with the FACT Act. Of course, credit unions may incorporate additional information that is not mentioned in the final Guidance, where appropriate.

Coordination With Credit Reporting Agencies

A trade association representing credit reporting agencies commented that its members are extremely concerned about their ability to comply with all of the duties (triggered under the FACT Act) that result from notices financial institutions send to their customers. This commenter strongly recommended that until a financial institution has contacted each nationwide consumer reporting agency to coordinate the timing, content, and staging of notices as well as the placement of fraud alerts, as necessary, a financial institution should refrain from issuing notices suggesting that customers contact nationwide consumer reporting agencies.

The commenter also stated that a financial institution that includes such suggestions in a notice to its customers should work with the credit reporting agencies to purchase the services the financial institution believes are necessary to protect its customers. The commenter stated that the costs of serving the millions of consumers it projects will receive notices under the proposed Guidance cannot be borne solely by the nationwide consumer reporting agencies.

The commenter also noted that the State of California has provided clear guidance in connection with its law requiring notice and also suggested that coordination with consumer reporting agencies is vital to ensure that a consumer can in fact request a file disclosure in a timely manner. This commenter stated that similar guidance at the federal level is essential.

The NCUA Board believes that the final Guidance addresses this commenter's concerns in several ways. First, for the reasons described earlier, the standard for member notice in the final Guidance likely will result in credit unions sending fewer notices. Second, the final Guidance does not require credit unions to send notices suggesting that consumers contact the nationwide consumer reporting agencies, in every case. Credit unions can use their discretion to determine whether such information should be included in a notice.

It is clear, however, that member notice may prompt more consumer contacts with consumer reporting agencies, as predicted by the commenter. Therefore, the final Guidance encourages a credit union that includes in its notice contact information for nationwide consumer reporting agencies to notify the consumer reporting agencies in advance, prior to sending large numbers of such notices. In this way, the reporting agencies will be on notice that they may have to accommodate additional requests for the placement of fraud alerts, where necessary.

Model Notice

Some commenters stated that if mandatory elements are included in the final Guidance, NCUA should develop a model notice that incorporates all the mandated elements yet allows credit unions to incorporate additional information where appropriate. Given the flexibility that credit unions now have to craft a notice tailored to the circumstances of a particular incident, the NCUA Board believes that any single model notice will be of little use. Therefore, the final Guidance does not contain a model notice.

Other Changes Regarding the Content of a Notice

The general discussion of the content of a notice in the final Guidance states that credit unions should give member notice in a ''clear and conspicuous manner.'' In addition, the final Guidance adopts a commenter's suggestion that credit unions should generally describe what the credit union has done to protect a member's information from further unauthorized access so that a member can make decisions regarding the credit union's member service. This addition allows a member to take measures to protect his or her accounts that are not redundant or in conflict with the credit union's actions.

The final Guidance also states that notice should include a telephone

number that members can call for further information and assistance. The NCUA Board added a new footnote to this text, which explains that the credit union should ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

Delivery of Customer Notice

NCUA received numerous suggestions regarding the delivery of member notice located in section II.D.3.a of the proposed Guidance. The proposed Guidance stated that member notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the member is likely to receive it. The proposed Guidance provided several examples of proper delivery and stated that a credit union may choose to contact all members affected by telephone or by mail, or for those members who conduct transactions electronically, using electronic notice.

One interagency commenter representing a large bank trade association agreed that this was a correct standard. However, many other commenters recommended that if it costs an institution more than $250,000 to provide notice to customers, if the affected class of persons to be notified exceeds 500,000, or if an incident warrants large distributions of notices, the final Guidance should permit various forms of mass distribution of information, such as by postings on an Internet web page and in national or regional media outlets. Commenters explained that the CDPA contains such a provision.[25]

One commenter suggested that a credit union should only provide notice in response to inquiries. By contrast, other commenters stated that the final Guidance should make clear that general notice on a web site is inadequate and that credit unions should provide individual notice to members.

The NCUA Board determined that the provision in the proposed Guidance that notice be delivered in a ''timely, clear, and conspicuous'' manner already appears elsewhere in the Guidance and is unnecessary here.

The NCUA Board has decided not to include a provision in the final Guidance that permits notice through a posting on the web or through the media in order to provide notice to a specific number of members or where the cost of notice to individual members would exceed a specific dollar amount. The Board believes that the thresholds suggested by commenters would not be appropriate in every case, especially in connection with incidents involving smaller institutions. Therefore, the final Guidance states that member notice should be delivered in any manner that is designed to ensure that a member can reasonably be expected to receive it. This standard places the responsibility on the credit union to select a method to deliver notice that is designed to ensure that a member is likely to receive notice.

The final Guidance also provides examples of proper delivery, noting that a credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive electronic communications from the credit union. Some commenters questioned the effect of other laws on the proposed Guidance. A few commenters noted that electronic notice should conform to the requirements of the Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. 7001 *et seq.* The final Guidance does not discuss a credit union's obligations under the E-Sign Act. The NCUA Board notes that the final Guidance specifically contemplates that a credit union may give notice electronically or by telephone. There is no requirement that notice be provided in writing. Therefore, the final Guidance does not trigger any consent requirements under the E-Sign Act.[26]

Still other commenters requested clarification that a telephone call made to a member for purposes of complying with the final Guidance is for ''emergency purposes'' under the Telephone Consumer Protection Act, 47 U.S.C. 227 (TCPA). These commenters noted that this is important because under the TCPA and its implementing regulation,[27] it is unlawful to initiate a telephone call to any residential phone line using an artificial or prerecorded voice to deliver a message, without the prior express consent of the called party, unless such call is for ''emergency purposes.''

The final Guidance does not address the TCPA, because the TCPA is interpreted by the Federal Communications Commission (FCC), and the FCC has not yet taken a position on this issue.[28]

V. Effective date

Many commenters suggested that NCUA include a transition period to allow adequate time for credit unions to implement the final Guidance. In accordance with applicable federal law, the final amendment to Part 748 is effective thirty days after publication in the **Federal Register**.

In addition, given the comments received, the NCUA Board recognizes that not every credit union currently has a response program that is consistent with the final Guidance. The Board expects these credit unions to implement the final Guidance as soon as possible. However, the Board appreciates that some credit unions may need additional time to develop new compliance procedures, modify systems, and train staff in order to implement an adequate response program. The NCUA Board will take into account the good faith efforts made by each credit union to develop a response program that is consistent with the final Guidance, together with all other relevant circumstances, when examining the adequacy of a credit union's information security program.

VII. Impact of Guidance

The NCUA Board invited comment on the potential burden associated with the member notice provisions for credit unions implementing the proposed Guidance. The Board also asked for information about the anticipated burden that may arise from the questions posed by members who receive the notices. In addition, the proposed Guidance asked whether NCUA should consider how the burden

[25] *See* CAL. CIV. CODE § 1798.82(g)(3) (West 2005).

[26] Under the E-Sign Act, if a statute, regulation, or other rule of law *requires* that information be provided or made available to a consumer in writing, certain procedures apply. *See* 15 U.S.C. 7001(c).

[27] 47 CFR 64.1200.

[28] NCUA notes, however, that the TCPA and its implementing regulations generally exempt calls made to any person with whom the caller has an established business relationship at the time the call is made. *See, e.g.,* 47 CFR 64.1200(a)(1)(iv). Thus, the TCPA would not appear to prohibit a credit union's telephone calls to its own members. In addition, the FCC's regulations state that the phrase for ''emergency purposes'' means calls made necessary in any situation affecting the health and safety of consumers. 47 CFR 64.1200(f)(2). *See also* FCC Report and Order adopting rules and regulations implementing the TCPA, October 16, 1992, available at *http://www.fcc.gov/cgb/donotcall/,* paragraph 51 (calls from utilites to notify customers of service outages, and to warn customers of discontinuance of service are included within the exemption for emergencies). Credit unions will give members notice under the final Guidance for a public safety purpose, namely, to permit their members to protect themselves where their sensitive information is likely to be misused, example, to facilitate identity theft. Therefore, the NCUA Board believes that the exemption for emergency purposes likely would include member notice that is provided by telephone using an artificial or prerecorded voice message call.

may vary depending upon the size and complexity of a credit union. The Board also asked for information about the amount of burden, if any, the proposed Guidance would impose on service providers.

Although many commenters representing credit unions stated that they already have a response program in place, they also noted that NCUA had underestimated the burden that would be imposed on credit unions and their members by the proposed Guidance. Some commenters stated that the proposed Guidance would require greater time, expenditure, and documentation for audit and compliance purposes. Other commenters stated that the costs of providing notice and requiring a sufficient number of appropriately trained employees to be available to answer member inquiries and provide assistance could be substantial. Other commenters stated that the Agencies failed to adequately consider the burden to members and customers who begin to receive numerous notices of ''unauthorized access'' to their data. They stated that the stress to members of having to change account numbers, change passwords, and monitor their credit reports would be enormous and could be unnecessary because the standard in the proposed Guidance would require notice when information subject to unauthorized access might be, but would not necessarily be, misused.

Some commenters maintained that the proposed Guidance would be especially burdensome for small credit unions, which one commenter asserted are the lowest risk targets. These commenters stated that the most burdensome elements of the proposed Guidance would be creating a general policy, establishing procedures and training staff. They added that developing and implementing new procedures for determining when, where and how to provide notice and procedures for monitoring accounts would also be burdensome.

Finally, a trade association commenter stated that the notice requirements in the proposed Guidance would impose a large burden on the nationwide consumer reporting agencies, over which they have no control and from which they have no means of recouping costs.

The NCUA Board has addressed the burdens identified by commenters as follows. First, the Board eliminated many of the more prescriptive elements of the response program described in the proposed Guidance. The final Guidance states that a credit union's response program should be risk-based. It lists a number of components that the program should contain.

Second, final Guidance does not detail the steps that a credit union should take to contain and control a security incident to prevent further unauthorized access to or use of member information. It also does not state that a credit union should secure all accounts that can be accessed using the same account number or name and password combination until such time as the credit union and the member can agree on a course of action. Instead, the final Guidance leaves such measures to the discretion of the credit union and gives examples of the steps that a credit union should consider, such as monitoring, freezing, or closing affected accounts. Thus, under the final Guidance a small credit union may choose to close an affected account, rather than monitoring the account, an element of the proposed Guidance that smaller credit unions identified as potentially very costly.

Third, though the final Guidance still states that notification to regulators should be a part of a credit union's response program, it states that notice should only be given when the credit union becomes aware of an incident of unauthorized access to or use of ''sensitive'' member information. This standard should result in fewer instances of notice to the regulators than under the proposed Guidance. The final Guidance also makes clear that when the security incident involves a service provider, the credit union may authorize the service provider to notify the credit union's regulator.

Fourth, the standard of notice to members also has been modified to be less burdensome to credit unions and their members. The NCUA Board believes that under this new standard, members will be less likely to be alarmed needlessly, and credit unions will no longer be asked to prove a negative—namely, that misuse of information is unlikely to occur. In addition, the Board also has provided credit unions with greater discretion to determine what should be contained in a notice to members.

The NCUA Board does not believe that there is a basis for exempting small credit unions from the Guidance. For example, many small credit unions outsource functions to large service providers that have been the target of those seeking to misuse member information. Therefore, the Board believes that all credit unions should prepare member response programs including member notification procedures that can be used in the event the credit union determines that misuse of its information about a member has occurred or is reasonably possible. However, as noted above, the Board recognizes that within the framework of the Guidance, a credit union's program will vary depending on the size and complexity of the credit union and the nature and scope of its activities.

Finally, to address comments relating to the potential burden on the nationwide consumer reporting agencies, as noted previously, the Guidance no longer suggests that member notice always include advice to contact the nationwide consumer reporting agencies. The NCUA Board recognizes that not all security breaches warrant such contacts. For example, the Board recognizes that it may not always be in the best interest of a consumer to have a fraud alert placed in the consumer's file because the fraud alert may have an adverse impact on the consumer's ability to obtain credit.

VIII. Regulatory Procedures

Paperwork Reduction Act

Certain provisions of the final Guidance contain ''collection of information'' requirements as defined in the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA). An agency may not conduct or sponsor, and a respondent is not required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number.

The NCUA Board requested comment on a proposed information collection as part of the notice requesting comment on the proposed Guidance. An analysis of the comments related to paperwork burden and commenters' recommendations is provided below. The NCUA submitted its proposed information collection to OMB for review and approval and the collections have been approved.

The NCUA Board has reconsidered the burden estimates published in the Proposed Guidance in light of the comments received asserting that the paperwork burden associated with the information collection were underestimated, and in light of measures taken to reduce burden in this final Guidance. The Board agreed to increase the estimate for the time it will take a credit union to develop notices and determine which members should be notified. However, revisions incorporated into the final Guidance will result in the preparation and issuance of fewer notices than was originally estimated. Therefore, the net change in burden is due to the rounding of numbers. A discussion of the

comments received follows the revised estimates.

New Estimates

Number of Respondents: 9,014.
Estimated Time per Response:

Developing Notices: 24 hours × 9,014 = 216,336 hours.

Notifying Customers: 29 hours × 153 = 4,437 hours.

Total Estimated Annual Burden = 220,773 hours .

Discussion of Comments

The information collection in the proposed Guidance stated that credit unions should: (1) Develop notices to members; and (2) determine which members should receive the notices and send the notices to members. The NCUA Board and the Banking Agencies received various comments regarding the burden estimates, including the estimated time per response and the number of recordkeepers involved.

Some commenters stated that the burden estimates of twenty hours to develop and produce notices and three days to determine which members should receive notice in the proposed Guidance were too low. These commenters stated that the Guidance should include language indicating that a credit union be given as much time as necessary to determine the scope of an incident and examine which members may be affected. One of these commenters stated that ten business days, as recommended by the California Department of Consumer Affairs Office of Privacy Protection, should provide a credit union with a known safe harbor to complete the steps described lest regulated entities be subject to inconsistent notification deadlines from the same incident.

These commenters misunderstood the meaning of PRA burden estimates. PRA burden estimates are judgments by the NCUA regarding the length of time that it would take credit unions to comply with information collection requirements. These estimates do not impose a deadline upon credit unions to complete a requirement within a specific period of time.

The final Guidance states that a credit union should notify members ''as soon as possible'' after an investigation leads it to conclude that misuse of member information has occurred or is reasonably possible. It also states that notification may be delayed at the written request of law enforcement.

The cost of disclosing information is considered part of the burden of an information collection. 5 CFR 1320.3(b)(1)(ix). Many commenters stated that the Agencies had underestimated the cost associated with disclosing security incidents to members pursuant to the proposed Guidance. However, these commenters did not distinguish between the usual and customary costs of doing business and the costs of the disclosures associated with the information collection in the proposed Guidance.

For example, one commenter stated that the Agencies' estimate did not include $0.60 per member for a one-page letter, envelope, and first class postage; the customer service time, handling the enormous number of calls from customers who receive notice; or the costs associated with closing or reopening accounts, printing new checks or embossing new cards. This commenter stated that printing and mailing costs, alone, for one notice to its customer database, at current postal rates, would be at least $500,000.

Some of the costs mentioned in this comment are non-labor costs associated with providing disclosures. Both NCUA and the Banking Agencies assumed that non-labor costs associated with the disclosures would be negligible, because institutions already have in place well-developed systems for providing disclosures to their customers. This comment and any other comments received regarding the Agencies' assumptions about non-labor costs will be taken into account in any future estimate of the burden for this collection.

Other costs mentioned in this comment, such as the cost of customer service time, printing checks, and embossing cards, are costs that the institution would incur regardless of the implementation of the final Guidance. These costs are not associated with an information collection, and, therefore, have not been factored into the NCUA Board's cost estimates.

In addition, the estimates in this comment are based on the assumption that notice should always be provided by mail. However, the final Guidance states that credit unions should deliver member notice in any manner designed to ensure that a member can reasonably be expected to receive it, such as by telephone, mail, or electronically for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically. The NCUA Board assumes that given this flexibility, credit unions may not necessarily choose to mail notices in every case, but may choose less expensive methods of delivery that ensure members will reasonably be expected to receive notice.

Another commenter concerned about the burdens imposed on consumer reporting agencies provided an example of a security breach involving a single company from which identifying information was stolen from about 500,000 military families. Among other things, the company's notice to its customers advised them to contact the nationwide consumer reporting agencies. The commenter stated that the nationwide consumer reporting agencies spent approximately $1.5 million per company, handling approximately 365,000 inquiries from the company's customers.

The final Guidance contains a number of changes that will diminish the costs identified by these commenters. First, the standard for notification in the final Guidance likely will result in fewer notices. In addition, the final Guidance no longer states that all notices should advise members to contact the nationwide consumer reporting agencies. Therefore, the NCUA Board estimates do not factor in the costs to the reporting agencies.

Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA) requires an agency to prepare a final regulatory flexibility analysis whenever the agency promulgates a final rule that may have a significant economic impact on a substantial number of small entities. As required by the RFA, the NCUA Board prepared and published an initial regulatory flexibility analysis at the time it issued the proposed rule amending § 748.0 and the proposed guidance in the form of Appendix B. This section contains the Board's final regulatory flexibility analysis.

A. Need for and Objectives of the Rule

As more fully discussed in the preamble to the final rule, section 501 of GLBA requires NCUA to publish standards for federally insured credit unions relating to their security programs to: (1) Insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. The final rule establishes that federally insured credit unions must include a response program as an element of their security program, and the final Guidance describes the features that a response program should contain to ensure that breaches of security do not

result in harm or inconvenience to members.

B. Summary of Issues Raised by Public Comment

The NCUA Board received no public comment specifically responding to the initial regulatory flexibility analysis contained in the proposed rule. All federally insured credit unions, regardless of size, are subject to GLBA and the rule. The Board believes the changes in the final Guidance, including the standard for determining when to provide notice to members and the increased emphasis on risk-based factors, make the final Guidance easier for smaller credit unions to use. For example, smaller credit unions that offer a relatively less sophisticated array of products and services present a relatively lower level of risk of security breach affecting member information. For these credit unions, the final Guidance contemplates a relatively less comprehensive response program, commensurate with the relatively lower level of risk. Another example of flexibility benefiting smaller institutions relates to service providers. The final Guidance contemplates that, where a service provider maintains member information, a credit union may delegate authority to that service provider to notify members affected by a security breach on its behalf. The Board believes this flexibility is of particular benefit to smaller credit unions, which typically use service providers and may not have the resources to provide timely and effective notice themselves.

C. Consideration of Alternatives

All federally insured credit unions are already required by GLBA and existing regulation to develop and implement a security program. Development of an effective program involves: Assessing risks to member information; establishing policies, procedures, and training to control risks; testing the program's effectiveness; and managing and monitoring service providers. The NCUA Board believes establishing an information security program is a sound business practice for all credit unions and is already addressed by existing supervisory procedures. The final rule requires that security programs include a provision for appropriate responses to incidents involving a breach of information integrity. Consistent with the position taken by the Banking Agencies, the Board views this as a fundamental element of any information security program. Members of smaller credit unions are entitled to expect their personal financial information will be protected and that their credit union will respond appropriately and effectively to any breach of security. Ultimately, there is no alternative to requiring that all credit unions include an effective response program as an element of their security programs.

Nevertheless, the Board specifically solicited comment in the proposed rule on any significant alternatives, consistent with GLBA, that would minimize the impact on small credit unions. As more fully discussed in the preamble to the final rule and in the preceding section of this analysis, the final Guidance provides substantial flexibility so that any credit union, regardless of size, may adopt an information security program tailored to its individual needs.

Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. The final rule would not have substantial direct effects on the states, on the connection between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined that this final rule does not constitute a policy that has federalism implications for purposes of the executive order.

The Treasury and General Government Appropriations Act, 1999—Assessment of Federal Regulations and Policies on Families

The NCUA has determined that this final rule would not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Public Law 105–277, 112 Stat. 2681 (1998).

Agency Regulatory Goal

NCUA's goal is to promulgate clear and understandable regulations that impose minimal regulatory burden. We invite your comments on whether the final rule is understandable and minimally intrusive.

List of Subjects in 12 CFR Part 748

Credit unions, Crime, Currency, Reporting and recordkeeping requirements and Security measures.

By the National Credit Union Administration Board on April 14, 2005.

Mary F. Rupp,

Secretary of the Board.

■ For reasons set forth in the preamble, the NCUA Board proposes to amend 12 CFR 748 as follows:

PART 748—SECURITY PROGRAM, REPORT OF CRIME AND CATASTROPHIC ACT AND BANK SECRECY ACT COMPLIANCE

■ 1.The authority citation for part 748 reads as follows:

Authority: 12 U.S.C. 1766(a), 1786(Q); 15 U.S.C. 6801 and 6805(b); 31 U.S.C. 5311 and 5318.

■ 2.In § 748.0 revise paragraph (b) to read as follows:

§ 748.0 Security program.

* * * * * *

(b) The security program will be designed to:

(1) Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

(2) Ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) Respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;

(4) Assist in the identification of persons who commit or attempt such actions and crimes, and

(5) Prevent destruction of vital records, as defined in 12 CFR part 749.

■ 3. Add Appendix B to read as follows:

Appendix B to Part 748—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

I. Background

This Guidance in the form of Appendix B to NCUA's Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance regulation,[29] interprets section 501(b) of the Gramm-Leach-Bliley Act (''GLBA'') and describes response programs, including member notification procedures, that a federally insured credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member. The scope of, and definitions of terms used in,

[29] 12 CFR Part 748.

this Guidance are identical to those of Appendix A to Part 748 (Appendix A). For example, the term ''member information'' is the same term used in Appendix A, and means any record containing nonpublic personal information about a member, whether in paper, electronic, or other form, maintained by or on behalf of the credit union.

A. Security Guidelines

Section 501(b) of the GLBA required the NCUA to establish appropriate standards for credit unions subject to its jurisdiction that include administrative, technical, and physical safeguards to protect the security and confidentiality of member information. Accordingly, the NCUA amended Part 748 of its rules to require credit unions to develop appropriate security programs, and issued Appendix A, reflecting its expectation that every federally insured credit union would develop an information security program designed to:

1. Ensure the security and confidentiality of member information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member.

B. Risk Assessment and Controls

1. Appendix A directs every credit union to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of member information; and

c. The sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.[30]

2. Following the assessment of these risks, Appendix A directs a credit union to design a program to address the identified risks. The particular security measures a credit union should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the credit union should consider the specific security measures enumerated in Appendix A,[31] and adopt those that are appropriate for the credit union, including:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to member information; and

c. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies.[32]

C. Service Providers

Appendix A advises every credit union to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.[33]

II. Response Program

i. Millions of Americans, throughout the country, have been victims of identity theft.[34] Identity thieves misuse personal information they obtain from a number of sources, including credit unions, to perpetrate identity theft. Therefore, credit unions should take preventative measures to safeguard member information against such attempts to gain unauthorized access to the information. For example, credit unions should place access controls on member information systems and conduct background checks for employees who are authorized to access member information.[35] However, every credit union should also develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems that occur nonetheless.[36] A response program should be a key part of a credit union's information security program.[37] The program should be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

ii. In addition, each credit union should be able to address incidents of unauthorized access to member information in member information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in this Guidance that relate to these arrangements, and with existing guidance on this topic issued by the NCUA,[38] a credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, a credit union's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused;

b. Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information as defined below.

c. Consistent with the NCUA's Suspicious Activity Report (''SAR'') regulations,[39] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;[40] and

e. Notifying members when warranted.

2. Where an incident of unauthorized access to member information involves member information systems maintained by a credit union's service providers, it is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

III. Member Notice

i. Credit unions have an affirmative duty to protect their members' information against

[30] *See* 12 CFR Part 748, Appendix A, Paragraph III.B.

[31] *See* Appendix A, paragraph III.C.

[32] *See* Appendix A, Paragraph III.C.

[33] *See* Appendix A, Paragraph III.B. and III.D. Further, the NCUA notes that, in addition to contractual obligations to a credit union, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (ldquo;FTC''), 12 CFR Part 314.

[34] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identify theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report,* (September 2003), available at *http://www.ftc.gov/os/2003/09synovatereport.pdf.*

[35] Credit unions should also conduct background checks of employees to ensure that the credit union does not violate 12 U.S.C. 1785(d), which prohibits a credit union from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1786(g).

[36] Under 12 CFR Part 748, Appendix A, a credit union's *member information systems* consists of all of the methods used to access, collect, store, use, transmit, protect, or dispose of member information, including the systems maintained by its service providers. *See* 12 CFR Part 748, Appendix A, Paragraph I.C.2.d.

[37] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December, 2002), available at *http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.htm1#infosec,* for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

[38] *See* FFIEC Information Technology Examination Handbook, Outsourcing Technology Services Booklet, (June 2004), available at *http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.htm1#outscouring* for additional guidance on managing outsourced relationships.

[39] A credit union's obligation to file a SAR is set out in the NCUA's SAR regulations and guidance. *See* 12 CFR Part 748.1(c); NCUA Letter to Credit Unions No. 04–CU–03, Suspiciouis Activity Reports, March 2004; NCUA Regulatory Alert No. 04–RA–01, The Suspicious Activity Report (SAR) Activity Review—Trends, Tips, & Isues, Issue 6, November 2003, February 2004.

[40] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, (December 2002), pp. 68–74.

unauthorized access or use. Notifying members of a security incident involving the unauthorized access or use of the member's information in accordance with the standard set forth below is a key part of that duty.

ii. Timely notification of members is important to manage a credit union's reputation risk. Effective notice also may reduce a credit union's legal risk, assist in maintaining good member relations, and enable the credit union's members to take steps to protect themselves against the consequences of identity theft. When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible. Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

1. Sensitive Member Information

Under Part 748.0, a credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member. Substantial harm or inconvenience is most likely to result from improper access to *sensitive member information* because this type of information is most likely to be misused, as in the commission of identity theft.

For purposes of this Guidance, sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account. *Sensitive member information* also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

2. Affected Members

If a credit union, based upon its investigation, can determine from its logs or other data precisely which members' information has been improperly accessed, it may limit notification to those members with regard to whom the credit union determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed. If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information is reasonably possible, it should notify all members in the group.

B. Content of Member Notice

1. Member notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of member information that was the subject of unauthorized access or use. It also should generally describe what the credit union has done to protect the members' information from further unauthorized access. In addition, it should include a telephone number that members can call for further information and assistance.[41] The notice also should remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the credit union. The notice should include the following additional items, when appropriate:

a. A recommendation that the member review account statements and immediately report any suspicious activity to the credit union;

b. A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;

c. A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the member may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.[42]

2. NCUA encourages credit unions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of members that include contact information for the reporting agencies.

C. Delivery of Member Notice

Member notice should be delivered in any manner designed to ensure that a member can reasonably be expected to receive it. For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

[FR Doc. 05–7836 Filed 4–29–05; 8:45 am]

BILLING CODE 7535–01–P

[41] The credit union should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to member inquiries and requests for assistance.

[42] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.ftc.gov/idtheft* and 1–877–IDTHEFT. The credit union may also refer members to any materials developed pursuant to section 15(1)(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).